Oct 19th, 2:00 PM - 2:50 PM

Why Managing 3rd Party Cybersecurity Risk is a Matter of National Security

Keith Deininger
SunTrust Bank, keith.a.deininger@suntrust.com

Why Managing 3rd Party Cybersecurity Risk is a Matter of National Security

How well are you assessing your 3rd party vendors security practices before giving them access to your data?

Keith A. Deininger

Digitally signed by Keith A. Deininger
DN: cn=Keith A. Deininger, o=SunTrust Banks, Inc., ou=ESR, email=keith.a.deininger@suntrust.com, c=US
Date: 2018.10.23 15:53:57 -04'00'

Presented by: Keith Deininger, CISSP, CISA
Senior Security Risk Analyst, Information Security Officer
Uber Big Bank (name withheld)

The legalese

Legal Mumbo-Jumbo

Disclaimer

The views and opinions expressed in this talk are my own and not those of my employer

All research was performed on personal time I am not here in representation of, or on behalf of, my employer

All information presented in this talk is designed to provide you the attendee with a greater understanding of the implications of ignoring due diligence with respect to Information Security Governance, Risk & Compliance in the workplace

WARNING: Those of you with an overwhelming fear of the unknown will be gratified to learn that there is no intended hidden message revealed by reading this disclaimer backwards

Thank you, Lawyer Cat

About myself

Keith Deininger

Senior Cyber Security Risk Analyst and
Information Security Officer
Uber Big Bank (name withheld)

- Education, let's just say it's a lot!
- 30 years IT with 15 years Cyber Security
- Certifications:
  - CISSP, CISA, and a whole lot more
- Avid Hacker of IoT devices and Maker of Things

- https://twitter.com/securitypro2704
- https://wwwlinkedin com/in/keithdeininger

The "Take-a-way's"

- Have a better understanding of Third-Party Vendor Relationship Risks and how to minimize them (risks that is)
- Learn some steps to mitigating Third-Party Vendor Risks; including how to *Identify* and *Assess* the risks
- Why every 3rd party vendor should not be treated equal when it comes to protecting your confidential data or IP
- Why insider threats from cybercriminals are perhaps the most serious threat to network Infrastructure or public system
- Finally… just have some fun learning about something new

So what about the title of the presentation?

KSU Proceedings on Cybersecurity Education, Research and Practice, Event 2 [2018]

https://digitalcommons.kennesaw.edu/ccerp/2018/industry/2

How can using the wrong 3rd party vendors be a risk to National Security?

Deininger, Why Managing 3rd Party Cybersecurity Risk is a Matter of National

(Rep's answers are on the board)

Electrical Power Grid , Water Treatment, Fuel Services – these are the biggest targets for cyber hackers Disrupt, disrupt, disrupt!

Banking & Financial Systems – "He who has the gold, makes the rules" – take someone's money away and watch the chaos that ensues

Ground Transportation Systems and Air Traffic Control systems – flying by wire and automated traffic controls

SCADA Attacks more common than you think

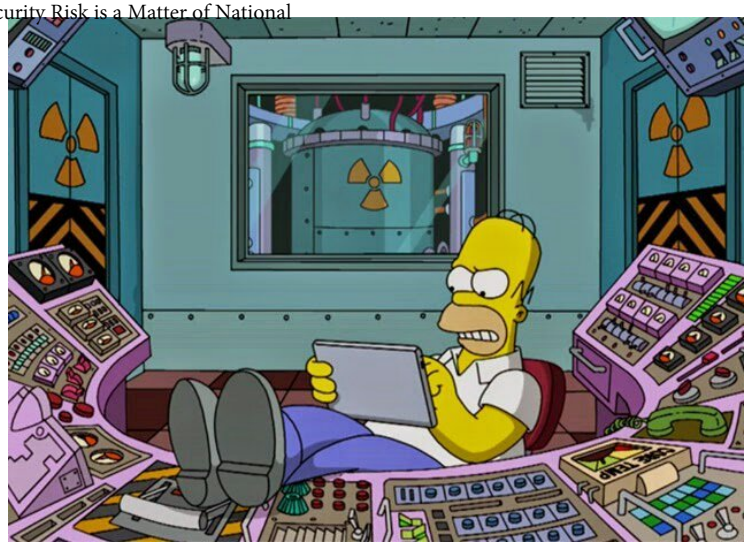
KSU Proceedings on Cybersecurity Education, Research and Practice, Event 2 [2018]

Cyber security threats are on the rise As a result, there is a focus on systems managing the critical infrastructure that everyone depends upon

"Critical infrastructure is loosely defined as assets essential for the economy and overall society to function "

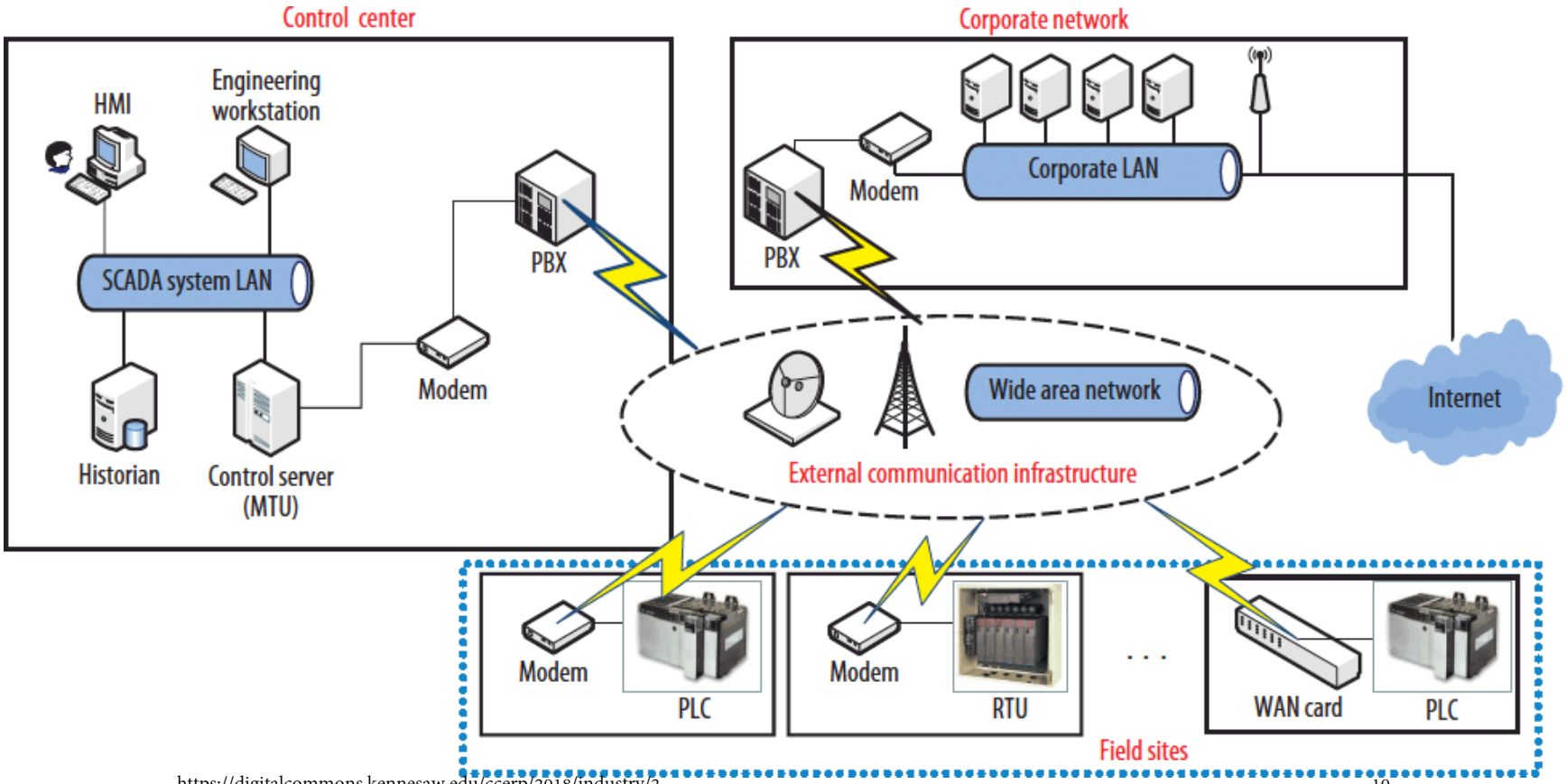
Just how susceptible are these systems to attack? Quite a bit more than most people think In the past the electrical grid and water treatment facilities were manned with onsite individuals, to streamline operations people were replaced with SCADA controllers

SCADA Systems



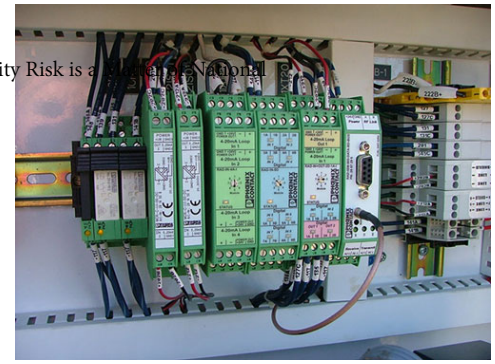
SCADA control systems

KSU Proceedings on Cybersecurity Education, Research and Practice, Event 2 [2018]



https://digitalcommons.kennesaw.edu/ccerp/2018/industry/2

SCADA control systems



SCADA Attacks

- Maroochy Shire (QLD) Sewage Spill (2000)
- Stuxnet attack on Iranian Uranium enrichment (2005-2015)
- CSX Train Signaling System (2008)
- Rye Brook, New York Dam Attack (2013)
- Unnamed German Steel Mill Attack (2014)
- Prykarpattyaoblenergo Control Center (PCC) (2015)
- IoT IP Cameras – Devil's Ivy Flaw (2017)

SCADA Attacks

- How are so many attacks happening?
  - Carelessness in manufacturing?
  - Inadequate due diligence assessments of service provider to uncover gaps in security
  - Not applying security patches and system upgrades
  - Insider threats from disgruntled employees
  - Malware and Phishing attacks are the easiest way to get a backdoor (C&C) inside a confined area
  - Worms attacks are still used to propagate attacks across as many connected systems as possible

Using 3rd Party Vendor Services in support of Critical Infrastructures

- Have a solidly built cyber security program
- Formal vendor management program
  - Thoroughly interview all 3rd and 4th party vendors
  - Ask "Do their practices align with our?"
  - If they are manufacturing products, strong Quality Control and Continuous Product Testing
- Use multiple vendors to provide similar services
  - Use more than 1 independent testing company
  - Rotate through your list of approved testing companies
- Follow a strict policy to replace EOL hardware and systems
  - This includes all servers, workstations, firewalls, PLC devices, etc.

Financial, Banking, Health & eCommerce/Retail Systems

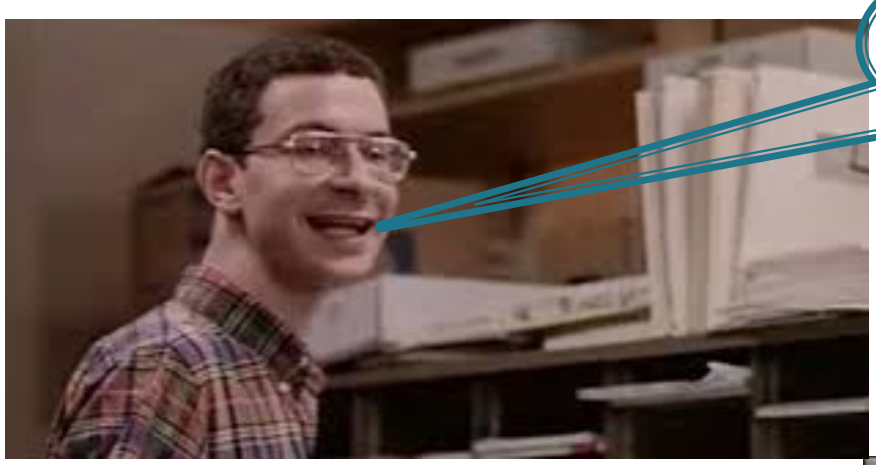
So let's examine banking and finance

- In the past few months it seems there have been more and more highly-publicized security breaches in the news)

- However, more often than not the culprit is found to be holes in the heads of the human operators and decision makers

- With many legacy banking systems, programmers included account backdoors to access systems without being traced using an admin account.

Why so many back doors?



Why so many back doors?

KSU Proceedings on Cybersecurity Education, Research and Practice, Event 2 [2018]

https://digitalcommons.kennesaw.edu/ccerp/2018/Industry/2 18

Banking and Retail IT Compliance

Banks and payment processors typically have to cover the costs of fraudulent charges to debit and credit cards in the wake of data breaches, even if they've taken the proper steps to protect customer data.

Item 3

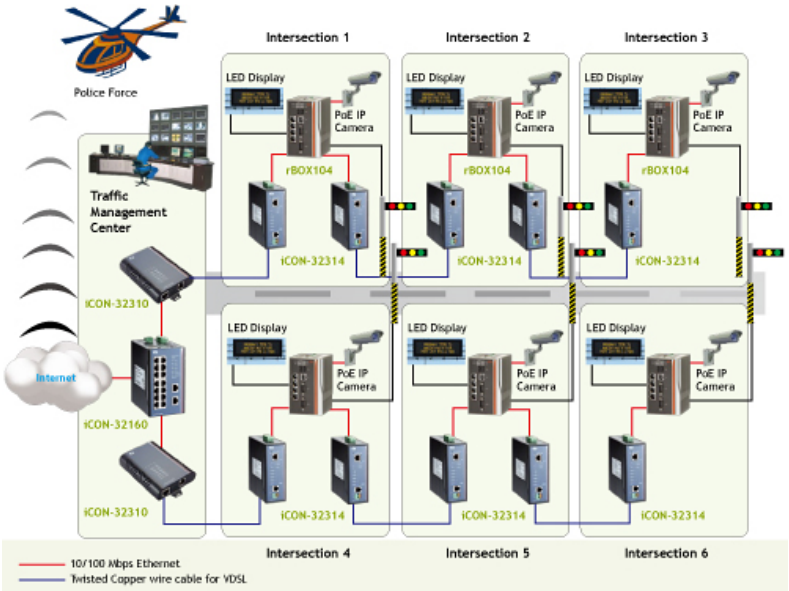
Handling 3rd Party Vendor Compliance

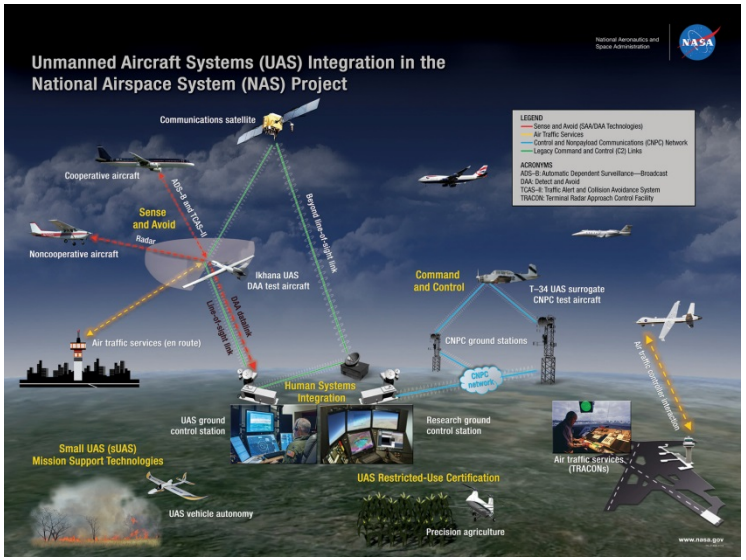
- In many instances, the very term "IT compliance" is a mystery to senior management
- Getting back to basic sound principles is key to help define the concept of EIG, and should be completed before exploring any further into issues of its abuse
- Same old thinking: "Our data is protected, we've never been breached yet So why change anything?"

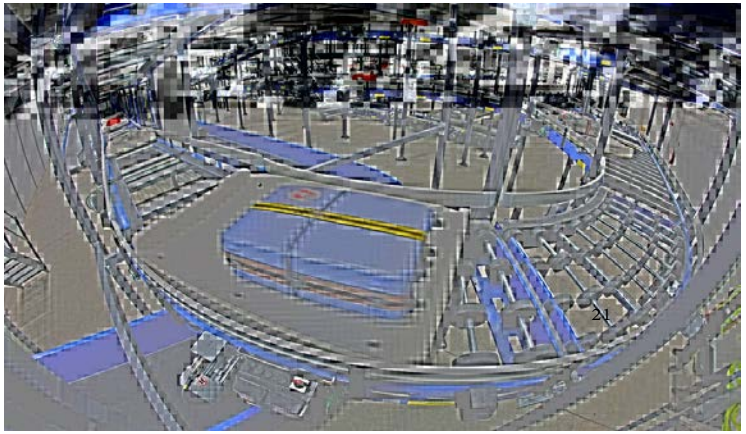
This is not how you want to drive your security compliance program

https://digitalcommons.kennesaw.edu/ccerp/2018/industry/2

Airlines and Transportation







Ground Transportation Systems and Air Traffic Control systems

- Delta made a discovery of a major data breach after the company that provides the airline's online chat services, 24/7.ai, had been involved in a cyber incident that last year compromised its own data security.
- Airlines are offering more connected services to patrons, but this comes a price. Hacking aircraft through the inflight entertainment systems has been proven beyond a doubt of possibility

Airline Industry Attacks through 3rd party vendor services

- British Airways online reservation systems were breaches and went unnoticed for several weeks.
- The compromised systems were compromised through a hacker gaining illicit access to the airline ticket processing servers.
- Forensics specialists suspect there was a backdoor account that was left by the 3rd party services provider.

Airport ground control systems – SCADA

- Airports use thousands of SCADA controlled devices throughout ground systems.
  - Baggage systems
  - Screening systems
  - Ground mapping systems
  - Facilities controls (Fire, CCTV, HVAC)
- Most airports use interconnected systems that all operate on the same network
  - Compromise one system and the rest will fall like dominos

Airport ground control systems – SCADA

Deininger: Why Managing 3rd Party Cybersecurity Risk is a Matter of National

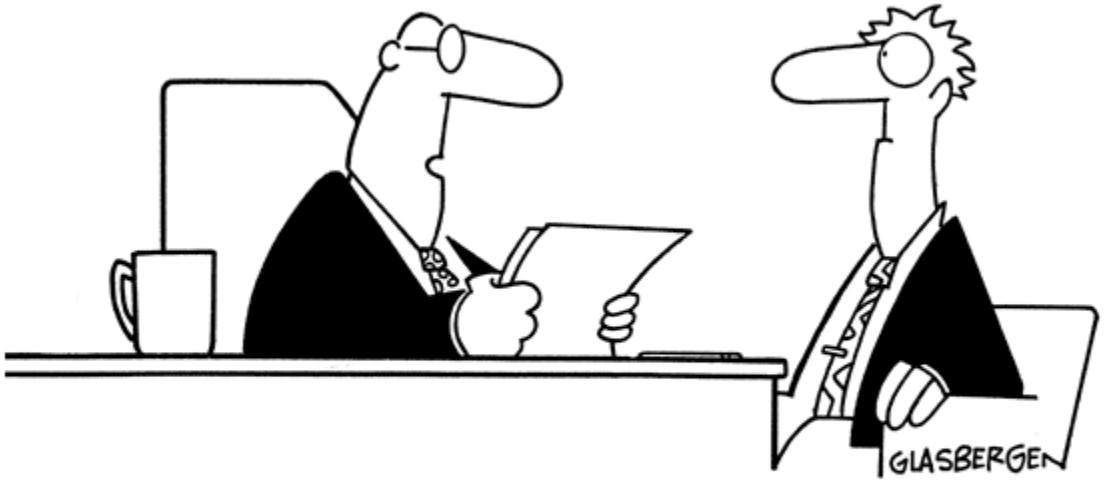
Why the huge concern?

- Increased scrutiny from the regulatory bodies, corporate boards and executive teams are more focused on governance related issues than ever before
- More companies are concerned over data breaches from 3rd and 4th party vendors and suppliers who may have carte-blanche access to networks and confidential private information
- Nobody wants to be known as “that company”

Integrated Risk Management

- Enterprise Risk
  - *Know where the vulnerabilities are and eliminate them if you can*
- Vendor Risk
  - *Who are your vendors? Do they practice strong data security?*
- Operational Risk
  - *Can your business recover from a breach in a timely manner?*
- Information Risk
  - *Do you really know where your data is at all times? Cloud – OPP*
- IT Risk
  - *When was the last time you practiced disaster recovery?*
- Corporate Compliance
  - *Have you truly reviewed your InfoSec policies lately?*
- IT Compliance
  - *Does your business understand regulatory issues it is susceptible to?*
- Security & Privacy
  - *What are you doing to protect your data while at rest and in transit?*
- Audit
  - *Could your company pass a SOC 2 Type II audit at this moment in time?*

Closing Remarks & Questions



"We're looking for someone who can help us crack down on identity theft. Fill out this application and don't forget to include your Social Security number, date of birth, phone number, home address and mother's maiden name."

Item 6

References and Citing

- Unknown owner, Public domain image of Lawyer Cat
- Homer Simpson, Created by Matt Groening for the Fox Broadcasting Company
- Dilbert cartoons, Copyright 2011, Created by Scott Adams, www dilbert com
- Unknown owner, Public domain image, www dealermarketing com
- The Interview, Copyright 2003, Created by Randy Glasbergen, www glasbergen com
- ISACA, Information Systems Audit and Control Association, www isaca org
- NIST, National Institute of Standards and Technology, www nist gov
- CIS, Center for Internet Security, https://www cisecurity org/